Office of the City Auditor

Vulnerability Assessment of the City's Computer Network

Report No. 0201

February 11, 2003

During this vulnerability assessment the outside consultant was not able to breach the City's network via a modem connection or the Intranet. This was not the case, however, once the consultant was provided access to an active network connection within a City facility. This report contains recommendations to address weaknesses that allowed the City's network to be compromised and steps that need to be taken to protect the data that is retained within the system.

"Most Livable City"

U.S. Conference of Mayors

OFFICE OF
CITY AUDITOR

7440 E. FIRST AVE
SCOTTSDALE, AZ 85251

(480) 312-7756 PHONE
(480) 312-2634 FAX

February 11, 2003

To the Most Honorable Mary Manross, Mayor
and Members of the Scottsdale City Council

Transmitted herewith is report No. 0201, the results of the second vulnerability assessment undertaken to evaluate the security of the City's computer network. This was a project on the 2002 annual plan for the Office of the City Auditor.

Canaudit, Inc., an independent consulting firm, conducted the assessment and, at the conclusion of the review, provided the City with details of what was found and the steps necessary to protect the City's network. These reports, "Network Vulnerability Assessment" and "Internet Penetration Audit," are reproduced in their entirety in this report as attachments One and Two. For security purposes, information such as internet protocol (IP) addresses and names of servers were replaced with pseudonymic data. In other instances, confidential data such as names, addresses, and passwords were redacted.

Information presented by the consultant was provided to the Information Systems Department for review. Management has reviewed the recommendations and has initiated corrective action as outlined in the action plan on page 4.

Because this assessment is the second evaluation of system security, this report also includes a summary of the recommendations outlined in 1999 and the current status of those recommendations. This summary is located on page 3.

If you need additional information or have any questions, please contact me at 480-312-7756.

Respectfully submitted,

Cheryl Barcala, CPA, CIA, CFE, CGFM, CISA, CISSP
City Auditor

EXECUTIVE SUMMARY

In 1999, the City conducted the first external vulnerability assessment of the City's computer network. The results of that assessment led the City to a commitment of additional funding for network security and the authorization for one dedicated staff position. City management also agreed to conduct, at least biennially, follow up assessments as a means of ensuring an adequate level of control. To that end, the City Council approved the inclusion of this project on the City Auditor's Audit Plan for 2001/2002. The work was conducted in accordance with generally accepted government auditing standards, with the exception of the requirement for peer review, as they relate to expanded scope auditing as required by Article III, Scottsdale Revised Code, §2-117 *et seq*.

The objectives of the assessment were to:

- Evaluate the City's network configuration.
- Test the firewalls.
- Review security practices currently in place.
- Evaluate the virtual private network (VPN) used for remote access to the network and the wireless cellular digital packet data (CDPD) connection used by staff in the field.
- Test modem connections.
- Evaluate the strength of passwords.

Canaudit, Inc. conducted the assessment in two stages. The first segment consisted of an external penetration test, conducted without prior notice, to evaluate the City's firewalls and intrusion detection systems. Prior to the completion of this segment, the consultant was not provided any information regarding the City's configuration.

The second segment was conducted while on-site using information gained during the external penetration stage. Canaudit was provided a work area, a personal computer with a CDPD connection, and access to an active network connection. Using freely available software, the consultant attempted to gain control of devices as well as harvest data.

At the conclusion of the assessment, Canaudit provided the City with two reports outlining the results of the tests performed. These reports, in their entirety, were provided to the Information Systems Department (IS).

Results in Brief

Canaudit was not able to compromise the City's network either through modem connections or the Internet. Staff in IS, responsible for monitoring the network, identified the attempts early in the penetration test, an indication that the firewall and intrusion detection system was working well. This early detection also limited the scope of the penetration test; once IS was aware that the test was underway, staff would scan the system and remove data placed by the consultant to facilitate the assessment.

While the consultant was not able to breach the City network remotely, this did not hold true once provided access to an active network connection. The first day, within a thirty-minute timeframe, several network devices had been compromised. During the five-day assessment period, Canaudit was able to gain administrative rights on 25 Microsoft NT systems and take control of a domain controller. In all, over 6,100 passwords were cracked. With compromised systems, the consultant was able to access e-mail accounts as well as harvest confidential information. Anyone who gains this ability could disrupt normal business operations or could create public relation situations designed to embarrass elected officials or employees.

Canaudit found inconsistent security on servers; many times a server with adequate security was located in close proximity (in network terms) to a server with weak security. This situation allowed the consultant to compromise more important servers by taking advantage of the ineffective security found on the less important servers. Canaudit also found simplistic passwords, default passwords that had not been changed, and in some situations, accounts where the password was the same as the user name.

Based on the severity of the issues identified, Canaudit recommends that the City invest in additional temporary resources to address the serious issues identified during the assessment.

Status of Recommendations – 1999 Vulnerability Assessment

No.	Recommendations	Management Response	Status
1.	The Chief Information Officer (CIO) should develop a citywide policy statement establishing a positive control environment and addressing aspects such as the code of conduct governing use and security of information system assets, management responsibility and user accountability, and management philosophy and direction regarding IS.	The *Information Systems Security Policy* document was developed for staff with technology related responsibilities. Administrative Regulation (AR) 136 addressing Network and Computer Security was developed for all City staff.	Complete
2	The CIO should create a full-time information system security position directed to implement a security program including:	This position was funded in fiscal year 2000/2001 and filled in December 2000.	Complete
	• Development of citywide security policies to ensure appropriate preventive measures, timely identification of errors or irregularities, limitation of losses, and timely restoration. This policy should address purpose and objectives, management structure, scope, assignment of responsibility, and penalties and disciplinary actions associated with failing to comply.	Administrative Regulation (AR) 136 *Network and Computer Security* and the *Information Systems Security Policy* have been adopted. This included a security cable lock and user awareness training video program for laptop users.	Complete
	• Development and implementation of an awareness program structured to communicate the security policy to all system users as a means of conveying the benefit of information system security to the organization, employees, and citizens. This awareness program should be supplemented with annual training to address security practices including ethical use of information system assets, and appropriate steps to protect against system failures and breaches.	A security awareness program has been initiated. It includes: • Security posters distributed bi-monthly. • Distribution of locks for portable computers and development of related training materials. • Expanded presence on Intranet. • Random security checks. • Articles in Cityline every 4-6 weeks. • Standard screensaver with security tips. In addition, a new online “Security Training” course will be used to educate staff about AR 136 beginning in February 2003.	Complete - Program has been initiated and will continue.

No.	Recommendations	Management Response	Status
	• Development and implementation of a monitoring program to detect attempted system intrusions.	IS has implemented several programs that monitor network traffic, plus firewall and server abnormalities. IS has also instituted resource reporting on File Transfer Protocol, Webmail, and remote network access (VPN & RAS).	Complete – Enhance-ments are ongoing.
	• Development of a CERT to appropriately address system security issues such as denial of service attacks and security breaches.	Information Systems technical staff has met to discuss security incident handling. Attended SANS conference track on Incident Handling in 8/2002. We have established our CERT (IS Security) team and identified their roles in an incident.	Complete
3	The CIO should develop a program to ensure independent vulnerability assessments at least biennially.	IS worked with the City Auditor's Office in planning for the second independent assessment, which was performed in July/August 2002. Funding for an independent vulnerability assessment will be included at least biennially in the IS budget. In the current budget process we are requesting $50,000 in funding, via an evaluation decision package, for outside biennial vulnerability assessments.	Complete

Action Plan

No.	Recommendations	Management Response	Status
The CIO should direct the IS Security Officer to implement the recommended corrective action to include:			
1	**Modem Issues**		
	• Review all modems currently in use within the City. For those in which a business need cannot be supported, remove the device.	1) AGREE – A review of City modems began in August 2002. We have documented and addressed the 56 modems identified by Canaudit. We have expanded the scope to include all 260 analog extensions in the City. These are being individually verified. Over 50 unused lines have been removed and this effort is now over 90% complete. Due to the individual onsite verification efforts often required, and sometimes-slow customer response, target completion has been revised to 2/24/03.	1) Underway - Target completion date 2/24/03
	• After review, develop a database with the location, purpose, and security level of all modems in use within the City.	2) AGREE – Construction of this database of modems is being done concurrently with item one above.	2) Underway - Target completion date 2/24/03
	• Develop a policy regarding appropriate security levels and periodically evaluate the status of modems. At a minimum, the policy should require: o Use of strong passwords. o Auto disconnect after three failed login attempts. o Use of encryption on confidentially transmitted information.	3) AGREE – Appropriate changes have been incorporated into the IS Security Policy. Also, we have purchased a licensed copy of the PhoneSweep product that performs both war dialing and system identification and penetration. This action has been added to the "Security Review Schedule."	3) Complete
2	**Unix and NT Issues**		
	• Ensure that default passwords are changed on all devices attached to the network.	1) AGREE – Default passwords have been identified and changed.	1) Complete
	• Ensure that NT security is fully implemented.	2) AGREE - Since the vulnerability assessment was conducted, we have migrated all of our network domain controllers to Windows 2000. This has allowed us remove the null session, implement	2) Complete for critical domain controllers Migration

No.	Recommendations	Management Response	Status
		NTLMv2, remove LM Hash codes, and setup standard account and security policies, plus implement standard audit policies that are controlled centrally and easily modified as needed. When the Windows 2000 migration is complete, all systems will have these settings in place.	underway for workstations and servers – target completion 12/1/03
	• Develop a citywide policy on hardening systems and ensure that the policy is implemented consistently throughout the organization.	3) AGREE – Standards documents for workstations and servers have been developed for Windows 2000.	3) Complete
	• Develop and implement a data classification scheme and require all resources to be labeled and protected according to risk.	4) AGREE – This is a major effort that will impact the entire organization and require substantial resources to implement.	4) Initial project definition and scope have begun – initial project plan to be ready 3/24/03
	• Restrict Domain Administrator access to the Police Department Windows server and require all sensitive data on the server to be protected.	5) DISAGREE – Our current support model requires IS system administrators be able to access all servers within the domain. Sensitive data will be classified and protected using planned "data classification" guidelines (see item 4).	5) No immediate action is planned
	• Require the UNIX umask to be set to 027 to prevent the accidental creation of a world readable or world writeable file.	6) AGREE – The default umasks have been changed.	6) Complete
	• Review and remove the rhosts files when possible. Set up empty rhosts files with no access permitted beyond root access.	7) AGREE – All of the "r" services and associate files have been removed or properly secured.	7) Complete
	• Implement the use of Secure Shell (SSH) in lieu of rlogin and rexec when a trust relationship is required.	8) AGREE – Using SSH is now our standard for making connections with Unix systems.	8) Complete

No.	Recommendations	Management Response	Status
	• Implement the use of TCP wrappers to restrict connections to trusted systems based on the source of the IP addresses.	9) AGREE – TCP wrappers have been implemented.	9) Complete
	• Review and disable TFTP, if possible.	10) AGREE – TFTP has been disabled.	10)Complete
	• Disable “verify” and “expand” commands on all systems running SMTP unless there is a proven need for these commands to be activated.	11) AGREE – These commands have been disabled except on the Library Alpha server. The Library system is scheduled to be replaced this year.	11)Complete
	• Implement a policy that requires the UNIX Administrator to undertake periodic reviews of passwords to enforce compliance with the City standard regarding password strength.	12) AGREE - This action has been added to the “Security Review Schedule.”	12)Complete
	• Disable the finger service on UNIX systems.	13) AGREE – Finger has been disabled.	13)Complete
	• Modify hosts equiv files to be root readable only.	14) AGREE – File masks have been updated.	14)Complete
	• Identify and remove any pre-TCB password files that are still maintained on HP-UX machines.	15) AGREE – pre-TCB files have been identified and removed.	15)Complete
	• Configure the Domain Name Servers (DNS) to respond to zone transfer requests only from authorized internal IP addresses.	16) AGREE – External name servers now only respond to requests from authorized IPs.	16)Complete
	• Disable use of null sessions, if NetBIOS must be used.	17) AGREE – Windows 2000 domain controllers, servers, and workstations no longer support null sessions.	17) Underway (see item 2)
	• Explore the possibility to restrict remote access to the registry to preclude the use of other tools to establish anonymous sessions.	18) With the changes made in the Windows 2000 environment, this will no longer be allowed.	18) Underway (see item 2)
	• Modify the password policy to require all accounts with administrative rights to force password changes every 15 days.	19) DISAGREE – We are planning to use two-factor authentication for improved administrator security.	19) Underway (see item 2)

No.	Recommendations	Management Response	Status
	• Develop and implement a remote access software policy to restrict the use of software such as PCAnywhere and VNC.	20) AGREE – Policies have been created for remote control and remote access. IS approval is required prior to any installation.	20)Complete
	• Create standardized account polices that: o Prohibit use of: ➢ "Password Never Expires." ➢ "Permit Blank Password."	21) a) AGREE – These are prohibited by policy.	21 a-c) Complete
	o Forcibly disconnect users logged on after appropriate business hours.	b) DISAGREE – To customize and maintain an individual schedule for all City staff is not reasonable. Our ten-minute keyboard lockout helps to mitigate this issue.	
	o Lock out accounts after repeated failed login attempts.	c) AGREE – Already in place.	
	o Require: ➢ Minimum password age to preclude users from manipulating the process to re-use passwords. ➢ Prohibit re-use of passwords within a 24-month period.	d) AGREE – A minimum password age will be established and reuse limited with a 24 month period.	21 d) Will complete by 2/24/03
	• Create a standard NT audit policy and establish responsibility for consistent reviews of activity.	22) AGREE - When Windows 2000 migration is complete, all systems will have a consistent audit policy.	22) Underway (see item 2)
3	**Network Devices**		
	• Adequately segment the network by using firewalls or routers with access control lists.	1) AGREE – The best approach to implementing this functionality and identifying specific hardware is under consideration as part of the overall network upgrade planned for this year.	1) Underway
	• Identify devices required to run SNMP and change the community strings to more difficult to guess words.	2) AGREE – SMTP has been removed where not needed and community strings have been changed as recommended.	2) Complete
	• Make the replacement of the SCO UNIX system a high priority to reduce the potential for a bottleneck at the core router.	3) AGREE – This will happen as part of the overall network upgrade planned for this year.	3) Underway

No.	Recommendations	Management Response	Status
4	**Wireless and CDPD Connections**		
	• Contact the service provider and request that the IP addresses be changed to non-routable.	1) AGREE – We have worked with the vendor to correct this issue.	1) Complete
	• Require all users to authenticate prior to being given Internet access.	2) AGREE – All users are now required to authenticate for Internet access.	2) Complete
	• If Internet access is granted, require use of software based personal firewalls.	3) AGREE – The CDPD connections are being moved under control of the City firewall.	3) Underway
	• Resolve, if possible, the unstable encryption when the signal strength drops.	4) AGREE – The CDPD vendor (Alltel) feels that the modem software incorrectly indicated the lack of encryption and has provided documentation from their equipment vendor to address the concern.	4) Complete
	• Explore the potential to require authentication prior to gaining access to the CDPD system.	5) AGREE – Additional authentication and network protection for CDPD devices is planned. (see item 3).	5) Underway
	• Explore the potential to require the third party vendor to limit access to information regarding the City's system.	6) This was researched with the CDPD modem manufacturer and determined to not be an issue.	6) Complete
5	**Police Department Computing Resources**		
	• Implement the use of Secure Socket Layer (SSL) or SSH instead of the rlogin service.	1) AGREE – The use of SSH protocol for Unix system connectivity is now a City standard.	1) Complete
	• Empty the rhosts file and restrict it sufficiently to ensure that it is only readable at root level.	2) AGREE – The rhosts file permissions have been changed as recommended.	2) Complete
	• Rename all Administrator accounts and set up a decoy "Administrator" account with a logon script set to notify the Security Administrator when attempts are made to gain access to the account.	3) AGREE – Our system administrators have developed this intrusion detection scheme, which is currently being deployed to servers.	3) Target completion is 3/31/03

No.	Recommendations	Management Response	Status
	• Identify and review the need for remote access connections. For those systems requiring remote access, require use of software with appropriate levels of security.	4) AGREE – PD remote access connections have been reviewed – software is set to require passwords and encryption.	4) Complete
	• Periodically review UNIX passwords by undertaking periodic audits of password strength.	5) AGREE - This action has been added to the "Security Review Schedule."	5) Complete
	• Determine the purpose of the netrc file and remove it, if possible.	6) AGREE – The netrc file is in use - access has been restricted to administrator (root) access.	6) Complete